Information Security Incident and Personal Data Breach Management Procedure

(Appendix 1 to Data Protection Policy)

Contents

Introduction

The risk of a security incident involving information, including personal data, held by organisations is significant. Cyberattacks, ransomware, phishing, malware, system and process failures, human error, lost or stolen devices are all examples of how data can be lost or compromised.

All incidents that may result in a breach of data protection regulations need to be recorded. Trafalgar Housing Association's Data Protection Lead will maintain a register of incidents and whether these have resulted in personal data breaches for Trafalgar Housing Association.

A security incident, resulting in a breach could damage Trafalgar Housing Association's reputation and our relationship with stakeholders or expose the organisation's staff and customers to the risk of fraud or identity theft. In addition, distress could be caused to the individuals concerned with the potential for legal action against Trafalgar Housing Association.

Some breaches must be reported to the Information Commissioners Office within 72 hours of us being made aware and in certain circumstances, there is also a need to notify the individuals whose personal data has been involved in the breach.

The Information Commissioner's Office has the right to impose enforcement notices on us or monetary fines (up to 4% of turnover) for breaches including the failure to notify a breach.

What is a Security Incident?

An information security incident is a suspected, attempted, successful, or imminent threat of unauthorised access, use, disclosure, modification or destruction of information; interference with information technology operations or significant violation of our acceptable use policy or information security policy.

Examples of information security incidents

- Computer system intrusion.
- Unauthorised access to premises where information is stored.
- Unauthorised or inappropriate disclosure of organisation information.
- Suspected or actual breaches, compromises, or other unauthorised access to Trafalgar Housing Association's systems, data, applications or accounts.
- Unauthorised changes to computers or software.
- Loss or theft of computer equipment or other data storage devices and media (laptop, USB drive, personally owned device used for work) used to store or access Trafalgar Housing Association's information.
- An attack that prevents or impairs the authorised use of networks, systems or applications.
- Interference with the intended use or inappropriate or improper usage of information technology resources.

A Security Incident involving personal data is considered a Personal Data Breach. If a security incident does not involve personal data, it will still be logged and investigated under this procedure.

What is a Personal Data Breach?

A personal data breach is a security incident leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It is important to understand that a personal data breach is more than just losing personal data. Whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches.

Roles and Responsibilities

All Staff

- Reporting any security incidents to the Data Protection Lead.
- Assisting with any investigation
- Implementing any actions to contain and recover information

Data Protection Lead (in conjunction with the Data Protection Officer as required)

- Recording all security incidents
- Deciding if incident has resulted in a personal data breach
- Manage investigations and actions to contain and recover information
- Notify the relevant staff, ICO and data subjects
- Identify lessons learned and implement actions to reduce future recurrence

Director and management Committee

- Ensure appropriate resources are allocated to assist in breach investigations, containment and recovery
- Review Breach Register and reports

Reporting a Security Incident

It is the responsibility of all staff to report any suspected or actual Security Incident as soon as possible to the Data Protection Lead including out of hours and at weekends. It is vital that the Data Protection Lead is notified of the incident promptly in order to ensure the necessary immediate actions are taken to reduce the impact of the incident and decide whether notification is required to the Information Commissioners Office (ICO) or data subject(s). Trafalgar Housing Association may also need to report the incident to the SHR.

Incidents/breaches should be reported to the Data Protection Lead by telephone and followed up with an email if you are unable to make direct contact via the phone. Where an incident involves electronic data or IT systems the Data Protection Lead will notify the IT Support Provider as soon as possible.

Containment & Recovery

An Incident requires investigation promptly to contain the situation and put in place a recovery plan to limit potential damage. The following needs to be established:

- Who is required to investigate the breach with the DPO and what resources will be required.

- Who needs to be made aware of the breach and what information do they need so they can assist in containing the breach. *(This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.)*
- Whether there is anything we can do to recover any losses and limit the damage the breach could cause. (*As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.)*
- If criminal activity is suspected the Police should be informed.

Assessing the Risks

Some data security incidents will not lead to risks beyond possible inconvenience to those who need the data to do their job. For example, where a laptop is irreparably damaged, but its files were backed up and can be recovered.

While these types of incidents can still have significant consequences, the risks are very different from those posed by, e.g. the theft of a tenant database when the data may be used to commit identity fraud.

The following should be considered when making an assessment:

- What type of data is involved? *If it includes personal data it will be considered a Personal Data Breach.*

- How sensitive is it? *Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details).*

- If data has been lost or stolen, are there any protections in place such as encryption?

- What has happened to the data? If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate or the organisation; if it has been damaged, this poses a different type and level of risk

- Regardless of what has happened to the data, what could the data tell a third party about an individual or the organisation? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.

- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment.

- Who are the individuals whose data has been breached? Whether they are staff or tenants will to some extent determine the level of risk posed by the breach and, therefore, the actions taken in attempting to mitigate those risks.

- What harm can come to individuals or the organisation? Are there risks to physical safety or reputation, or financial loss or a combination of these?

- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service we provide?

- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

Notification to ICO

The ICO should be notified (by the Data Protection Lead or DPO) when the breach is likely to result in a risk to the rights and freedoms of individuals. If unaddressed, such a breach is likely to have a significant detrimental effect on individuals, e.g. it may result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Incidents, and whether to notify the ICO, need to be assessed on a case by case basis. For example, the ICO should be notified about a loss of personal data where the breach leaves the data subjects open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list would not normally meet the threshold for notification. Enclosure 1 to this procedure provides examples of breaches that require notification and to whom.

The decision to notify the ICO will be made by the Data Protection Lead with advice from the DPO. The decision and thinking behind it will be recorded in the Breach Register and/or incident file. Notification will be made online using the ICO's form and will include:

- The nature of the personal data breach including, where possible: the categories and approximate number of individuals concerned; and the categories and approximate number of personal data records concerned.

- The name and contact details of the Data Protection Officer or other contact point where more information can be obtained.

- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

A notifiable breach has to be reported to the ICO within 72 hours of us becoming 'aware' of it. When we become 'aware' of the breach is the point when we know or suspect there has been a personal data breach. We may not discover that a security incident is a personal data breach initially, but as soon as we do know or suspect that personal data is involved then we are 'aware'. Some examples to help determine when we become aware:

- In the case of a loss of a CD or data stick with unencrypted data it is often not possible to ascertain whether unauthorised persons gained access. Nevertheless, in most cases, this should be notified as there is a reasonable degree of certainty that a breach has occurred; we would become 'aware' when we realised the CD or data stick was missing.
- A third party informs us that they have accidentally received the personal data of a tenant and provides evidence of the unauthorised disclosure. As we have been presented with clear evidence of a breach then there can be no doubt that we have become 'aware'.

- We detect that there has been a possible intrusion into our IT network. We check our systems to establish whether personal data held on that system has been compromised and confirm that this is the case. Once again, we now have clear evidence of a breach there can be no doubt that we have become 'aware'.

It is recognised that it will often be impossible to investigate a breach fully within the 72 hour time-period and legislation allows for us to provide information to the ICO in phases.

We should always aim to notify the ICO as soon as possible even if we do not have much detail at that point. However, for initial notifications delayed beyond 72 hours, the reasons for the delay in notification should be given.

Notification to Data Subjects

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we must notify those concerned directly and without undue delay, unless this would involve disproportionate effort.

If it is not possible to contact the data subjects directly or there are a large number of data subjects involved, then we should make a public communication or similar measure whereby the data subjects are informed in an effective manner. Dedicated messages must be used when communicating a breach to data subjects and they should not be included in other information such as regular updates or newsletters. This helps make the communication of the breach clear and transparent. Examples of transparent communication methods include direct messaging (email, SMS), prominent website banners, social media posts or notification, postal communications and prominent advertisements in printed media.

Communicating a breach to data subjects allows us to provide information on the risks presented as a result of the breach and the steps the data subjects can take to protect themselves from its potential consequences. When notifying the data subjects of a breach, we must provide the following information:

- a description of the nature of the breach;
- the name and contact details of the Data Protection Lead and/or DPO;
- a description of the likely consequences of the breach; and
- a description of the measures taken or proposed to be taken by us to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.
- Who the data subject should contact if they require further information or if they wish to make a complaint. This should include the ICO's details.

Evaluation/Lessons Learned

It is important not only to investigate the causes of the breach and learn lessons from it but also to evaluate the effectiveness of our response. If it was identified that the breach was caused, even in part, by systemic problems, then simply containing the breach and continuing 'business as usual' is not acceptable. If management of the breach was

hampered by inadequate policies or procedures, these policies and procedures must be reviewed and updated to prevent a recurrence. The Data Protection Lead and DPO should conduct the evaluation with relevant staff involved in the breach and conduct the necessary training to ensure that the lessons are learned.

Records Management

A Security Incident and Breach Register will be maintained by the Data Protection Lead and this will be reported to the Management Committee on a regular basis. A case file or folder should be created for each incident containing a full record of the incident, relevant correspondence, decisions on notifications and investigation/evaluation. Records should be retained as per the Trafalgar Housing Association Retention Schedule.

Review of Procedure

This procedure will be reviewed every 12 months or more frequently when required to address any weakness in procedures or changes in legislation or best practice.

Enclosures:

1. Notification Guidance.
2. ICO Form – Report a Personal Data Breach.
3. Template Breach Register.

Enclosure 1 – Notification Guidance

(Taken from Article 29 Working Group adopted guidance)

Examples of personal data breaches and who to notify.

The following non-exhaustive examples will assist in determining whether we need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	Notify the ICO	Notify the Data Subject(s)	Notes
A controller stored a backup of an archive of personal data encrypted on a CD. The CD is stolen during a break-in	No	No	As long as the data are encrypted with a state of the art algorithm, backups of the data exist, and the unique key is not compromised, this may not be a reportable breach. However if it is later compromised, notification is required
Personal data of individuals are infiltrated from a secure website managed by the controller during a cyber-attack.	Yes, report to ICO if there are potential consequences to individuals	Yes, depending on the nature of the personal data affected and if the severity of the potential consequences to individuals is high	If the risk is not high, we recommend the controller to notify the data subject, depending on the circumstances of the case. For example, notification may not be required if there is a confidentiality breach for a newsletter related to a TV show, but notification may be required if this newsletter can lead to political point of view of the data subject being disclosed
A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No	No	This is not a notifiable personal data breach, but still a recordable incident. Appropriate records should be maintained by the controller
A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that	Yes, report to the ICO, if there are potential consequences to individuals as this is a loss of availability	Yes, depending on the nature of the personal data affected and the possible effect of the lack of availability of the	If there was a backup available and data could be restored in good time, this would not need to be reported to the ICO or to individuals as there would have been no permanent loss of availability or confidentiality. However, the ICO may consider an investigation to assess compliance with the broader security requirements

there was no other malware present in the system		data, as well as other likely consequences	
An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and if it is a systemic flaw so that other individuals are or might be affected	Yes	Only the individuals affected are notified if there is high risk and it is clear that others were not affected	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them
Personal data of 5000 students are mistakenly sent to the wrong mailing list with 1000+ recipients	Yes	Yes, depending on the type of personal data involved and the severity of possible consequences	
A direct marketing e-mail is sent to recipients in "to:" or "cc:" field, thereby enabling each recipient to see the email address of other recipients	Yes, notifying the ICO may be obligatory if a large number of individuals are affected, if sensitive data are revealed	Yes, depending on the type of personal data involved and the severity of possible consequences	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.